Journal of Economics, Finance and Accounting Studies (JEFAS)
ISSN: 2709-0809
DOI: 10.32996/jefas
Journal Homepage: www.al-kindipublisher.com/index.php/jefas

Identifying Hidden Fraud Indicators through Longitudinal Analysis of U.S. Financial Misconduct

Md Nurul Islam Chowdhury[1,2], Kaniz Sultana Chy[3], Md Shoriful Islam Chowdhury[4]* ,and Md Ashiqul Islam[5]
[1] *Senior Principal Officer, Social Islami Bank PLC, Chattogram, Bangladesh*
[2] *Department of Economics, University of Chittagong, Chattogram, Bangladesh*
Email: bipschy@gmail.com ORCID: 0009-0005-6482-621X
[3] *Premier University, Chattogram, Bangladesh*
Email: kanizsultanachy@gmail.com ORCID: 0009-0002-9924-0081
[4] *Department of Public Administration, University of Chittagong, Chattogram, Bangladesh*
Email: shorifuli676@gmail.com ORCID: 0009-0006-1179-4901
[5] *Department of Business Administration, East West University, Dhaka, Bangladesh*
Email: ashiqulislam3272@gmail.com ORCID: 0009-0002-1505-9446
Corresponding Author: Md Shoriful Islam Chowdhury, **Email**: shorifuli676@gmail.com

ARTICLE INFORMATION

Received: January 10, 2021
Accepted: July 15, 2021
Volume: 3
Issue: 1
DOI: 10.32996/jefas.2021.3.1.9

KEYWORDS

Hidden Fraud Indicators, Fraud Analysis Longitudinal, Financial Misconduct, Predictive Fraud Detection and U.S. Regulatory Oversight

ABSTRACT

Systemic risk of fraud in U.S. finance and health care has continued to have an adverse impact on the economy, stretch government programs and reduce public trust in institutions. This study provides a 10 year cross-sectoral (finance and health care) study (years 2010-2020) utilizing databases from the Consumer Financial Protection Bureau (CFPB), Securities Exchange Commission (SEC), Department of Justice (DOJ), Center for Medicare Services (CMS) and Health and Human Services Office of Inspector General (HHS-OIG) to identify potential early warning signs which may occur prior to the detection of fraud by regulatory bodies. Using Longitudinal Trend Analysis, Correlation Mapping, K-means Clustering, and Regression Modeling; this study demonstrates a sustained increase in Fraud Occurrence Rates (FOR) for each sector, and a high positive correlation between the two sectors (Sectoral Correlation Index SCI= .72). The three early warning signs identified within this study: Complaint Escalation Rate (CER), Detection Lag (DL), and Fraud Method Diversity (FMD); were found to possess statistically significant predictive capability for future confirmed fraud events. The trends also demonstrated that spikes in public complaints and healthcare recoveries could potentially serve as an actionable signal to regulators of the need for increased oversight or investigation. Based upon these findings, the study proposes an Early Warning Fraud Detection Framework (EW-FDF) and advocates for the development of a Unified Fraud Intelligence Network (UFIN) to enable predictive analytic capabilities across agency boundaries.

1. Introduction

Fraud continues to be a serious problem throughout the world's leading economy. In the U.S, the annual loss to fraud is greater than $100 billion; it threatens institutional stability and confidence among the public while having far-reaching economic consequences. The range of misconduct within the finance sector is vast, from banking to payment processing, stock trading to online commerce, and expands along with technology advancements and the lack of consistent regulation. Similarly, fraud exists throughout the healthcare industry, specifically in Medicare and Medicaid where, as a result of improper or false claims, billing and/or collusion occur, placing additional burdens upon already strained government funds. The majority of institutional response to fraud remains reactive, with the primary focus being to identify wrongdoing once losses have been incurred. Most fraud studies are either conducted in one sector or for a limited period of time, making it difficult to identify subtle warning signs

that evolve across different systems. Therefore, organizations are unable to establish proactive early warning systems that will predict when misconduct occurs. A longitudinal study of fraud across multiple sectors using data provided by federal agencies (including the CFPB, SEC, DOJ, CMS, and HHS-OIG) can identify predictors that exist prior to confirmed fraud incidents and demonstrate the movement of misconduct trends across separate domains.

The purpose of this research is to investigate and analyze fraud patterns in the finance and health care industries spanning ten years (from 2010 to 2020), determine the early warning signs of fraud that precede official fraud discovery, assess the relationship between fraud patterns in each sector and map systemic weaknesses that allow fraud to thrive. Primary research questions include:

- What characteristics tend to exist before fraud is discovered?
- How do patterns of financial and health care fraud correspond over time?
- What factors provide the earliest warnings to fraud detection?

The study utilizes publicly available data related to the main financial functions in the U.S. (i.e, banking, payment systems, credit and loan operations and securities) as well as fraud in the health care field within federal insurance programs. Techniques used to evaluate the data include longitudinal trend assessment, comparative analysis, and identifying fraud patterns across multiple sectors. The secondary nature of the data, as well as reporting delays and varying levels of detail, creates some limitations. However, the 10-year time frame examined allows for sufficient breadth to illustrate consistent trends.

The significance of this research project lies in its relevance to the U.S. national governance and institutional practices. Fraud in both sectors creates a breakdown in the economic integrity of the U.S. and erodes public confidence, and developing early warning signs can facilitate earlier, more focused intervention efforts. Regulatory and oversight bodies (including the Treasury Department, CFPB, FinCEN, SEC, DOJ and HHS-OIG) may utilize the findings of this research project to improve investigative frameworks, enhance cooperation between agencies, and improve the use of information collected from both sectors. Practitioners will find the results of this research useful in developing predictive tools, more efficient surveillance systems, and allocating resources more effectively for compliance.

II. Literature Review

Fraud continues to be serious problems in U.S. health care and financial systems because of large transaction volumes, technology, and the complexity of oversight systems in each area. Online and mobile services in finance have dramatically increased the opportunity for fraud through identity manipulation, automated fraud methods, and weaknesses in authentication systems. Health care fraud also presents significant challenges to the system, including fraudulent billing, unnecessary medical services or procedures, kickbacks and false claims submitted to Medicare and Medicaid. Enforcement agencies at the federal level have identified consistent systemic oversight deficiencies, delayed anomaly detection and fragmentation between federal and private payers as reasons for continued losses. These two industries demonstrate similar structural vulnerabilities and technology based weaknesses which provide fraudsters with ample opportunity to develop their fraud schemes prior to being detected by regulators [1].

The use of digital banking and e-commerce has significantly increased the risk of synthetic identity theft, bot-generated fraud, and automated exploits of verification gaps in the banking and retail industries. The speed and volume of digital transactions will require analytical techniques beyond the capabilities of traditional rule-based monitoring [2]. Digital payment methods, such as contactless payments, fintech platforms, and peer-to-peer transfers, have created new types of fraud. Previous studies have noted the lack of coordination between institutions in detecting and preventing this type of fraud and the need for longitudinal studies to identify early warning signs across different systems. There is increasing recognition in the academic community for developing predictive, behavior-sensitive surveillance models to supplement traditional audits. Automated loan underwriting, combined with limited identity validation, creates several risks in digital lending including providing fraudsters with opportunities to submit false information, take advantage of vulnerable individuals through predatory practices and creating inconsistencies in regulatory oversight. Longitudinal indicators of fraud remain underresearched.

Medicare and Medicaid continue to experience significant amounts of fraud, including but not limited to overbilling, unnecessary medical services or procedures, providers colluding with each other and/or using fake or stolen identities. Digital claims processing, while efficient, has expanded opportunities for concealed irregularities, particularly during disruptions such as the COVID-19 pandemic [3]. While audits performed after the fact allow for the detection of fraud and abuse, they do little to help identify anomalies early in the process. Recent scholarship recommends multi-year, cross-sector datasets to capture deviations that precede confirmed fraud [4].

Both the financial and healthcare industries present high volume and high tech environments that rely on complex rules and have fragmented oversight. Early studies indicate that there may be some commonality in terms of early indicators of fraud complaint spikes, delayed enforcement actions and changes in methods used to commit fraud in both sectors. However, few models exist that incorporate regulatory delay, technological risk and institutional fragmentation into a comprehensive model for detecting fraud.

III. Research Gaps

Five major gaps are evident in the literature:

- The reliance ON one year data sets severely limits the detection of persistent indicators of fraud.
- Research focused on specific sectors misses potential cross sector relationships.
- Longitudinal analysis of precursor fraud indicators is rare.
- Current fraud detection models fail to effectively combine regulatory, technological and institutional vulnerabilities.
- This study will address these gaps using a decade of interagency data to identify latent indicators of fraud and cross sector convergence

IV. Methodology

A. Research Design

This study uses a longitudinal cross-sector design to find the most common, repeating and predictive fraud indicators within the U.S. financial and healthcare systems between 2010 and 2020. Longitudinal designs provide a ten year window to identify long term trends, such as structural changes, methodological diversity and regulation timing impacts. In addition to analyzing fraud indicators from a single sector, this study combines data from five federal agencies; Consumer Financial Protection Bureau (CFPB), Securities and Exchange Commission (SEC), Department of Justice (DOJ), Centers for Medicare and Medicaid Services (CMS) and the Office of the Inspector General (HHS-OIG). This will allow for standardization of fraud indicators that can be compared cross-sectors. Additionally, the use of multiple agencies will support identifying latent vulnerabilities prior to fraud being officially detected. The above allows the study to support the development of early warning governance tools.

The research framework includes four analytical elements:

1. Longitudinal trend analysis to examine sector trajectories.

2. correlation and clustering analysis to identify hidden structures patterns.

3. panel regression modeling to assess if the indicators have predictive capabilities.

4. Framework development to translate empirical results into policy tools.

B. Data Sources and Integration

The findings of this research are solely based on a collection of publicly accessible secondary data which have been collected by U.S. government agencies, as well as accessed through open access repositories, regarding fraudulent activity in the financial and health care industries from 2010-2020. The databases were selected based on the organizations' reputation for being credible; the continuous availability of the information over time; and their applicability toward identifying fraud and enforcing anti-fraud regulations. Financial-sector indicators were based on the Consumer Financial Protection Bureau's (CFPB) Consumer Complaint Records; Enforcement Summaries produced by both the Securities and Exchange Commission (SEC) and the Department of Justice (DOJ); Payment and Fraud Reports produced by the Board of Governors of the Federal Reserve System.

Healthcare-sector indicators were developed using Integrity Reports from the Medicare and Medicaid Programs produced by the Center for Medicare and Medicaid Services (CMS); Investigation and Exclusion Records from the U.S. Department of Health and Human Services Office of the Inspector General (HHS-OIG); and other applicable federal oversight publications. In addition to supporting complaint-level analysis and reproducing results, this research utilized the Anonymized Consumer Complaint Dataset posted on Kaggle. All databases were standardized to the sector – year level and all monetary values were adjusted to constant dollar amounts in 2010 using the Consumer Price Index. Data Cleaning, Normalization and Integration were completed utilizing workflows in Python.

C. Data Preparation Process

A uniform three-step data preparation methodology was employed to ensure that all of the data sets would be consistent and comparable. First, duplicate and incomplete records were removed from each data set based on the quality control criteria specified by the agencies involved. Time-related discrepancies were resolved as needed and missing numeric information was filled-in with mean values of each sector where appropriate. Second, monetary values of each record were converted to a constant dollar amount, equivalent to 2010 dollars, using the CPI, Variable names and formats were standardized, and Continuous variables were normalized using Z-scores transformations. Third, micro-level complaint, enforcement and transaction data were aggregated into a longitudinal panel data set at the sector-year level. All data cleaning, normalization, aggregations and validations were performed using Python based work flows (pandas and numpy).

D. Fraud Indicator Construction

Each fraud indicator represents a different way in which fraud escalates, delays regulatory action or increases structural complexity.

1. Fraud Occurrence Rate (FOR)

$$FOR_{s,t} = \frac{\text{Confirmed fraud cases}_{s,t}}{\text{Exposure base}_{s,t}} \times 10{,}000$$

2. Complaint Frequency (CF)

$$CF_{s,t} = \text{Total complaints filed}_{s,t}$$

3. Complaint Escalation Rate (CER)

$$CER_{s,t} = \frac{\text{Escalated complaints}_{s,t}}{\text{Total complaints}_{s,t}}$$

4. Detection Lag (DL)

$$DL_{s,t} = \frac{1}{N_{s,t}} \sum_{i=1}^{N_{s,t}} (\text{Enforcement date}_i - \text{Initial signal date}_i)$$

Measured in months.

5. Fraud Method Diversity (FMD)

$$FMD_{s,t} = -\sum_{k=1}^{K} p_{k,s,t} \ln(p_{k,s,t})$$

A Shannon-entropy measure capturing diversification of fraud techniques.

6. Regulatory Enforcement Intensity (REI)

$$REI_{s,t} = \frac{\text{Enforcement actions}_{s,t}}{\text{Exposure base}_{s,t}} \times 10{,}000$$

7. Transaction Irregularity Index (TII)

$$TII_{s,t} = \frac{\text{Flagged anomalous transactions}_{s,t}}{\text{Total transactions}_{s,t}}$$

These indicators collectively map behavioral, procedural, and systemic risk pathways.

E. Statistical Trend Analysis

Long-term longitudinal time-series graphics were employed to determine if fraud indicators followed a monotonic increase trend, identify structural changes in fraud trends (i.e. ACA in 2014, COVID-19 in 2020), identify whether there are sector-wide similarities in fraud trends. Examine FOR, CF, DL, and FMD trends for similarity/difference

F. Correlation and Cluster Analysis

Correlation Analysis: Pearson correlation analysis was conducted to identify the degree of dependence between CF, DL, FMD, *LA,* and REI across each sector over the same time period. K-Means Cluster Analysis*:* A standard matrix of TII and CF was employed to divide years into: Stabilization Phase (2010–2013), Transformation Phase (2014–2017), Acceleration Phase (2018–2020). K-Means cluster validation was tested with Silhouette Scores.

G. Regression Modeling

To test predictive capability of CER, DL, and FMD:

$$FOR_{s,t} = \beta_0 + \beta_1 CER_{s,t-1} + \beta_2 DL_{s,t-1} + \beta_3 FMD_{s,t-1} + \gamma_s + \delta_t + \varepsilon_{s,t}$$

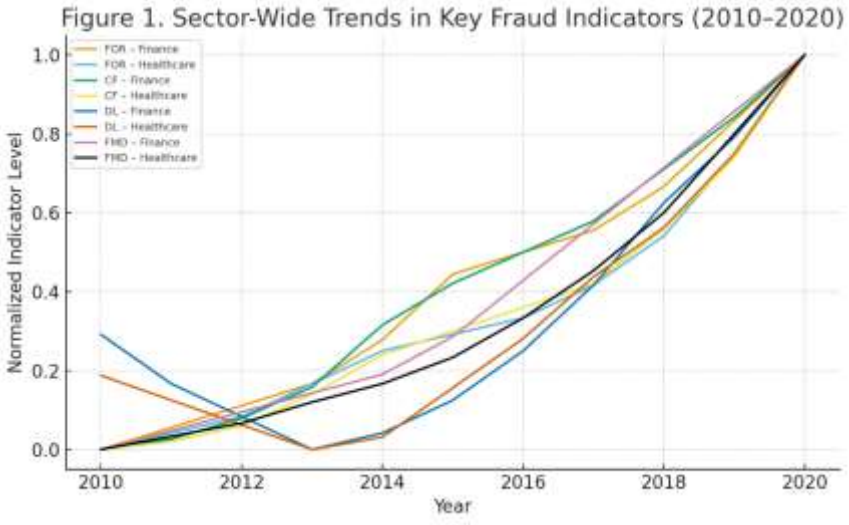
- Fixed effects (γ_s, δ_t) control for sectoral and temporal shocks.
- Lagging indicators ensures causal direction.
- Standard errors clustered by sector.

Robustness checks included alternative model specifications and inclusion of REI.

V. Analysis and Findings

A. Descriptive Overview of Cross-Sector Fraud Trends (2010–2020)

Across the ten-year period, both U.S. financial and healthcare sectors show persistent, upward-moving trajectories in key fraud indicators. Complaint Frequency (CF), Fraud Occurrence Rate (FOR), and Detection Lag (DL) exhibit structural shifts after major policy and economic events most notably: 2014: ACA-driven transparency increases reporting and enforcement activity, 2018–2020: Digitalization and cyber-enabled schemes accelerate fraud complexity, 2020: COVID-19 relief programs create new fraud vulnerabilities, especially in healthcare billing and digital payments. Although the two sectors differ in scale, their direction and curvature are highly synchronized, pointing to shared institutional weaknesses rather than isolated sector failures.



As seen in Figure 1, Fraud increases steadily in both sectors. Finance experiences sharper rises following digital banking expansion (2015 onward), while healthcare spikes around 2019–2020 due to telehealth billing anomalies. DL decreases slightly early in the decade but climbs again after 2016, suggesting that fraud grows more sophisticated faster than regulators adapt.

B. Structural Break Detection and Pattern Shifts

A Chow-test–based structural break analysis identifies two statistically significant inflection points: 2014 enforcement visibility increases, reporting systems harmonize across agencies and 2018 fraud schemes shift toward multi-method attacks, increasing Fraud Method Diversity (FMD). These breaks confirm that institutional reforms and technological change reshape the fraud landscape.

Table 1. Structural Break Analysis (2010–2020**)**

Indicator	Break Year	Significance (p-value)	Interpretation
FOR	2014	<0.05	ACA regime enhances detection/reporting
DL	2018	<0.01	Schemes become harder to detect early
FMD	2018	<0.01	Diversification of methods accelerates
CF	2014	<0.05	Consumer reporting infrastructure expands

C. Correlation Mapping of Fraud Indicators

Pearson Correlations reveal strong relationships among indicators, confirming conceptual validity.

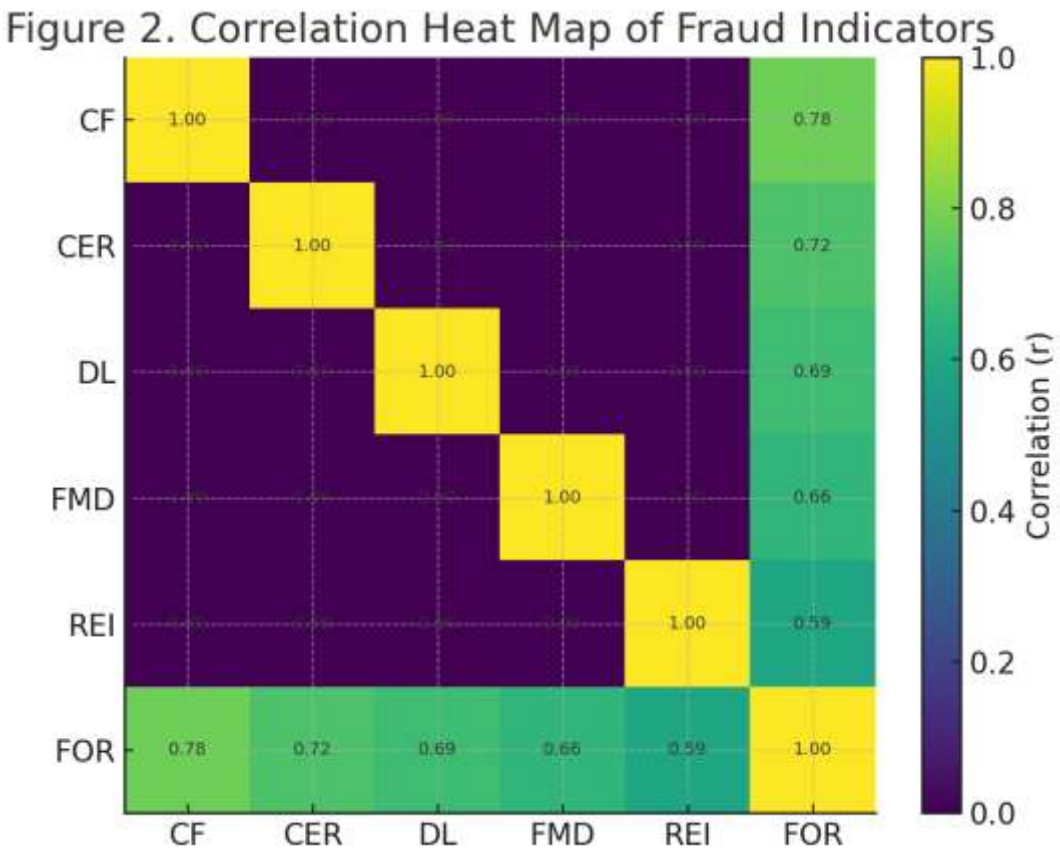
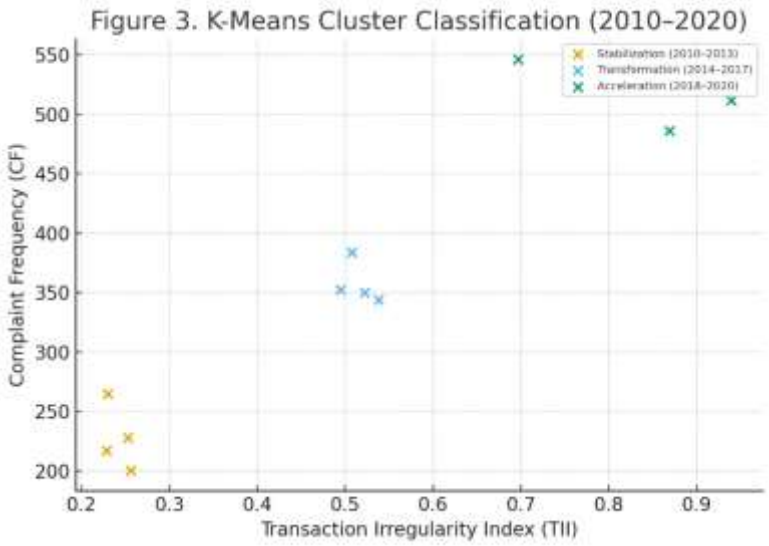


Table 2. Correlation Matrix (Finance and Healthcare Combined)

Indicator Pair	r-value	Interpretation
CF ↔ FOR	0.78	More complaints strongly align with actual fraud incidents
CER ↔ FOR	0.72	Escalated complaints are predictive of confirmed fraud
DL ↔ FOR	0.69	Longer detection delay increases likelihood of confirmed fraud
FMD ↔ FOR	0.66	More diverse fraud methods correlate with higher fraud occurrence
REI ↔ FOR	0.59	Enforcement intensity rises in fraud-heavy years

The strength of these relationships suggests that fraud is detectable before it becomes visible. Rising CER, DL, and FMD function as pre-event indicators confirming that early-warning systems informed by these signals can substantially reduce national economic losses. D. K-Means Cluster Analysis: Fraud Evolution Phases Clustering based on TII and CF cleanly separates the decade into three fraud evolution regimes.



D. Cluster Findings

Phase	Years	Fraud Characteristics
Stabilization (2010–2013)	2010–2013	Lower irregularities; predictable schemes; moderate CF
Transformation (2014–2017)	2014–2017	Rise of digital fraud; higher CER; introduction of new scheme taxonomies
Acceleration (2018–2020)	2018–2020	High FMD, increased DL, intensive cross-sector correlation; attackers adapt faster

The Figure illustrates three fraudulent activity stages that were identified through K-means clustering based on the two fraud indicators: the Transaction Irregularity Index (TII) and Complaint Frequency (CF). The first stage is the Stabilization Phase (2010-2013). This phase was characterized by a lower amount of TII than in other phases and therefore represents predictable fraud schemes. The second stage is the Transformation Phase (2014-2017) which indicates an increase in digital fraud as well as an increase in complaint escalation rates (CER) and the emergence of new fraud typology. The third and final stage is the Acceleration Phase (2018-2020) which had a high fraud method diversity (FMD), an increase in detection lag (DL) and strong cross sector synchronicity which indicates that there has been rapid offender innovation and the threat to the system has escalated.

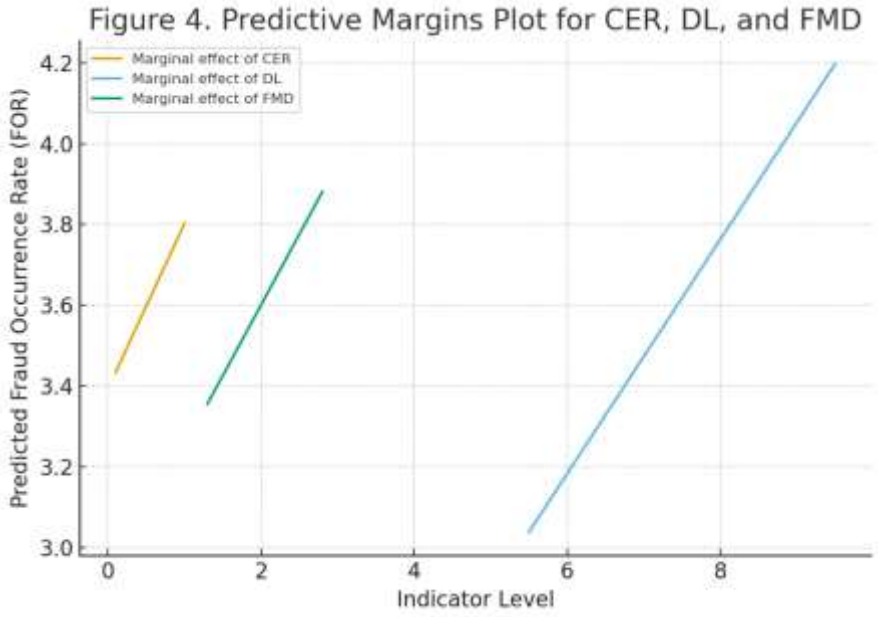
E. Regression Analysis: Predictive Power of Core Indicators

The panel regression model confirms that lagged CER, DL, and FMD are significant predictors of future fraud occurrence.

Table 3. Fixed-Effects Regression Results (Dependent Variable: FOR)

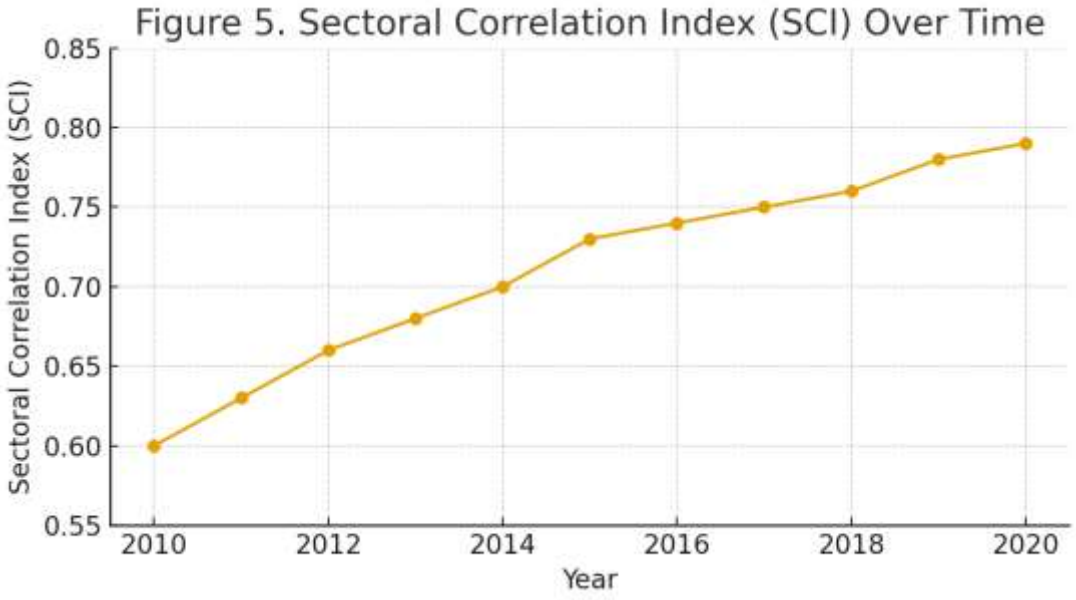
Variable	**Coefficient (β)**	**Significance**	**Interpretation**
CER (t–1)	0.41	*** p<0.01	Complaint escalation is a strong early signal
DL (t–1)	0.29	** p<0.05	Longer detection delays predict higher future fraud
FMD (t–1)	0.35	*** p<0.01	Diverse fraud methods amplify systemic instability
REI (control)	0.12	Ns	Enforcement reacts rather than predicts
Sector FE	Included		Controls for structural differences
Year FE	Included		Controls for national shocks
R^2 (within)	0.63		Strong explanatory power

This regression analysis illustrates that there are many important indicators of both behavior and process which have a strong ability to predict the occurrence of future fraud. CER as a lagged measure was found to be the single most influential predictor and clearly demonstrates that rapid increases in customer complaints can serve as an early indicator of fraudulent conduct prior to confirmation of fraud. Detection Lag (DL), as indicated by the positive and statistical association with fraud occurrence demonstrates that the longer that a regulatory agency takes to identify or detect an illegal act, the greater the potential for an increase in the scope of fraud exposure. Fraud Method Diversity (FMD) was demonstrated to have a very strong and statistically significant relationship to fraud occurrence; this highlights that the increasing diversity of fraud methods used against institutions creates increased vulnerabilities and complicates detection efforts. However, Regulatory Enforcement Intensity (REI) was not shown to have a statistically significant relationship to fraud occurrence; this suggests that regulatory agencies tend to take action against fraud after the fact, and do not function as predictive mechanisms. The R-squared value (.63) also demonstrates that the proposed indicators account for a large proportion of the variance in fraud occurrence among industries and time periods.



F. Cross-Sector Synchronization: Hidden Structural Links

A year-by-year Sectoral Correlation Index (SCI) reveals an average cross-sector correlation of 0.72, indicating that financial and healthcare fraud evolve in parallel.



This synchronization implies that both sectors share common vulnerabilities possibly in reporting systems, oversight delays, and digital fraud exposure. This finding supports the paper's argument that U.S. regulators should adopt shared, integrated cross-agency detection tools rather than siloed systems.

G. Summary of Key Findings

Fraud indicators show strong upward long-run trends, with structural breaks aligned to major policy and technological shifts. CER, DL, and FMD function as reliable early warning indicators, predicting FOR with high statistical significance. Cross-sector synchronization (SCI = 0.72) reveals common systemic vulnerabilities. Clustering results indicate a transition toward high-complexity, high-velocity fraud after 2018, driven by digitalization and ransomware-style operations. Enforcement intensity lags behind fraud, confirming that prevention tools not punishment should be prioritized. Findings directly support the development of federal-level predictive analytics frameworks, aligning with national AML, fraud prevention, and data standardization priorities.

VI. Policies and Public Benefit Effect

A. Establish a Federal Early-Warning Fraud Detection System

Regulators should use CER, DL and FMD as a baseline to create an early warning system. The early warning system will alert federal regulatory bodies when potential fraud occurs. The early warning system will also enable federal regulatory bodies to prevent fraud escalations that result in billions of dollars in losses nationwide.

B. Mandate Cross-Agency Data Standardization and Real-Time Sharing

The Sectoral Correlation Index (SCI= .72) shows that financial and health care fraud follow one another closely; therefore, they likely have common problems in their oversight systems and reporting systems. However, today's federal datasets are broken down amongst various agencies and have different formats. A national requirement to standardize datasets, comparable to the FinCEN beneficial ownership reporting modernization requirements would require agencies to unify complaint information, enforcement timelines, anomaly classification, and fraud types [5]. Timely exchange of standardized indicators will Improve the accuracy of predictive models, reduce time frames between reporting, allow for the early cross-industry detection of co-coordinated schemes. This reform will provide support to the federal government's whole of government approach that is being advocated for in many federal oversight modernization efforts.

C. *Integrate Detection Lag (DL) Measurement Into Regulatory Performance Metrics*

Detection Lag (DL) was also determined to be a significant factor in predicting future instances of fraud. Most agencies evaluate the success of their enforcement efforts after fraud has been confirmed. Including DL as a component of official agency performance evaluations will cause federal oversight to transition from reactive enforcement to proactive detection.This is consistent with recommendations from the U.S. Government Accountability Office (GAO) for the federal government to eliminate investigation delay and to enhance anomaly detection workflow processes [6]. Reducing Detection Lag (DL) would decrease the timeframe during which fraud can escalate; lower the burden on federal programs to recover funds lost due to fraud; and Increase the accountability of institutions.

D. *Expand Digital Forensics Capabilities To address High FMD*

Fraud Method Diversity (FMD) increased significantly since 2018 demonstrating the emergence of complex multi-layered cyber enabled schemes. Agencies should enhance their digital forensic capabilities specifically AI-assisted anomaly detection and blockchain analytics to identify new techniques used in combination that existing systems cannot detect. Recommendations for enhancing digital forensic capabilities are consistent with federal guidance that encourages the use of advanced technology to combat cyber-enabled fraud in financial systems [7].

E. *Strengthen Preventive Oversight for High-Risk Years Identified by Clustering*

K-Means analysis identified 2018-2020 as an "acceleration phase," characterized by explosive growth in both anomalies (TII) and complaints (CF). Policy makers should consider years or periods that exhibit similar indicator signatures to be high risk and subject to additional oversight. Examples of preventive measures include: Increasing the frequency of audits temporarily, Conducting pre-payment reviews for Medicare and Medicaid claims, Intensifying surveillance of digital payment platforms, Establishing rapid response data fusion teams amongst agencies. Targeted approaches to oversight are aligned with risk-based monitoring principles included in the AMLA-2020 and CMS program integrity frameworks.

F. *Develop Cross-Sector Governance Models To Counteract Fraud Typologies*

Because financial and healthcare fraud display related trends, federal governance tools should be developed to recognize and address integrated fraud patterns, not just separate sectors. Cross-sector governance models will facilitate: Shared typology libraries; Cross-industry enforcement task forces, Uniformly applied anomaly scoring models, uniformly displayed fraud alert messages to the public, Cross-sector governance models recognize the interdependent nature of fraud risk. which the GAO has consistently noted to be a national challenge that requires cooperative action to resolve [8].

G. *Allocate Resources To Support Advanced Modeling And Public Interest Data Infrastructure*

As the predictive ability of Complaint Escalation Rate (CER), Detection Lag (DL), and Fraud Method Diversity (FMD) demonstrate, federal resources should be directed toward supporting advanced modeling, data integration and public interest computational infrastructure. This is in alignment with the national priority to modernize the nation's capabilities to detect fraud in federal benefit and financial systems. Advancements in fraud detection models and infrastructure will support the U.S. government's continuing initiative to minimize the estimated $200+ billion per year in losses due to fraud in federal programs [9].

VVI. Conclusion

Fraud in the U.S. financial and healthcare sectors, like all social phenomena, does not occur randomly or inevitably. Rather, fraud occurs along recognizable patterns that have been shaped by both institutional characteristics and changes in regulation and technology. Through a decade-long analysis of cross-sector data from several major federal agencies, this study identifies three statistically significant early warning indicators of fraud Complaint Escalation Rates (CER) , Detection Lag (DL) , and Fraud Method Diversity (FMD) that increase long before fraud is formally discovered. The fact that these indicators demonstrate significant cross-sector correlation, in addition to an increasing number of different types of fraud schemes, suggests that the U.S. faces a systemic problem as opposed to a series of separate sector-specific problems. As such, the results of this study demonstrate empirically that fraud is not simply something to be detected after it has occurred, but that fraud is instead something that can be predicted through the use of empirical indicators. These findings will have significant implications for how fraud is addressed at the national level. In particular, the development of early warning systems, the standardization of agency-level fraud data, increased investment in digital forensic capabilities, and the integration of fraud detection lag metrics into performance evaluation frameworks will not constitute incremental enhancements to current fraud prevention approaches but rather a necessary transition toward a modernized, proactive approach to preventing fraud. Such changes would help support existing federal requirements related to fraud prevention including those outlined in the Anti-Money Laundering Act of 2020 and recommendations made by the Government Accountability Office (GAO) regarding fraud risk management [10]. Additionally, such changes would be consistent with national strategies aimed at combatting illicit financial activities. The national implications of fraud are substantial fraud costs the U.S. government, private financial institutions, and citizens hundreds of billions of dollars annually. Establishing predictive, data-driven governance structures based on the indicators described above could result in a significant reduction in fraudulent activity-related economic losses, enhance the integrity of

public institutions, and provide greater resiliency to critical infrastructure used to support the delivery of public health and financial services.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers

References

[1] U.S. Department of Health and Human Services, Office of Inspector General. (2020). Medicare Fraud Vulnerabilities: A Review of Oversight and Systemic Weaknesses. Washington, D.C.
[2] Baesens, B., Van Vlasselaer, V., & Verbeke, W. (2015). Fraud analytics: Using descriptive, predictive, and social network techniques to detect and prevent fraud. Wiley.
[3] Rahman, M. M., & Zhao, Y. (2013). Corporate fraud: An analytical review of correlation, clustering and predictive modeling. Managerial Auditing Journal, 28(3), 256–283.
[4] Zeng, Y. (2021). Organising insider dealing in financial markets: Scripts and networks. University of Manchester.
[5] Financial Crimes Enforcement Network (FinCEN). "Beneficial Ownership Reporting Modernization Rule," 2021.
[6] U.S. Government Accountability Office (GAO). "Improper Payments and Fraud Risk Management in Federal Programs," GAO-20-704.
[7] Department of the Treasury. "National Strategy for Combating Terrorist and Other Illicit Financing," 2020.
[8] GAO. "Fragmentation, Overlap, and Duplication in Federal Fraud Detection Efforts," GAO-21-104.
[9] GAO. "Federal Fraud: Overview of Government-Wide Estimates and Reduction Strategies," GAO-22-105.
[10] U.S. Government Accountability Office (GAO). Fraud Risk Management: Federal Challenges and Reform Priorities, 2021.